分布式 SOM 结合 K-均值聚类的软件定义网络泛洪攻击检测方法 *

汪海涛 [1]，余松森 [2]

(1. 广东科贸职业学院 信息与自动化学院，广州 510620; 2. 华南师范大学 软件学院，广东 佛山 528225)

摘　要：针对软件定义网络（SDN）泛洪攻击导致的上层性能瓶颈和过载问题，提出一种分布式自组织映射（DSOM）结合 K-均值聚类的网络流量攻击检测方法。首先，位于应用层的 DSOM 控制器将现有数据集发送给集成了 DSOM 扩展包的交换机，在每个交换机上分别训练 DSOM 映射；然后，在预定时间内合并 DSOM 映射；最后，DSOM 控制器将合并后的 DSOM 映射发送到所有 OpenFlow 交换机，利用 K-均值聚类完成最终的分类。实验结果表明，DSOM 方案能够有效检测异常流量、解决瓶颈问题，相比传统方法具有一定的优势。此外，提出的方法提高了系统对攻击流量的反应速度，同时给网络系统带来较小的开销。

关键词：软件定义网络；泛洪攻击；分布式自组织映射；K-均值聚类；OpenFlow

中图分类号：TP393.08　　doi: 10.3969/j.issn.1001-3695.2018.06.0401

Software-defined network flooding attack detection method based on distributed SOM and K-means clustering

Wang Haitao[1], yu Songsen2

(1. *College of Information & Automation Guangdong Polytechnic of Science & Trade*, *Guangzhou* 510620, *China*; 2. *School of Software*, *South China Normal University*, *Foshan Guangdong* 528225, *China*)

Abstract: Aiming at the problem of performance bottleneck and overload in upper layer caused by software-defined network flooding attacks, this paper proposed a software-defined network flooding attack detection method based on distributed SOM and k-means clustering. The DSOM controller at the application layer first sent the existing data set to the switch which had the DSOM extension package integrated and it trained the DSOM mapping on each switch. Then, it consolidated the DSOM mapping within a predetermined time. Finally, the DSOM controller sent the merged DSOM mapping to all OpenFlow switches and used k-means clustering to complete the final classification. Experimental results show that the DSOM scheme can effectively detect abnormal traffic and solve bottleneck problems, which has certain advantages over traditional methods. In addition, the proposed method improves the response speed of the system to attack traffic and at the same time it brings less overhead to the network system.

Key words: software-defined network; flooding attacks; distributed self-organizing map; K-means clustering; OpenFlow

0　引言

软件定义网络（software defined network，SDN）[1]是一种优秀的网络架构模型。在 SDN 中，控制层和数据层的分离为网络运营商在流量管理方面带来了巨大的好处。OpenFlow 协议[2]是 SDN 中的一个主要组件，它是 SDN 控制器和 OpenFlow 交换机之间的通信者。SDN 控制器使用 OpenFlow 协议，根据安全和路由策略等网络业务指令，配置和更新 OpenFlow 交换机内部的流表。

在 OpenFlow 交换机数量较多的大型网络中，由于安全服务和应用程序的资源分配，SDN 控制器自然而然成为性能瓶颈。

另外，在流量大的情况下，数据层与控制层之间的通信通道可能也会成为瓶颈，使得延迟增加并且会阻碍到应用层的流量[3]。因此，许多研究人员为大型软件定义网络引入了多个控制器，比如谷歌的 B4 网络[4]等。在遇到泛洪攻击或分布式拒绝服务（DDoS）攻击[5,6]时，上述问题将成为大型 SDN 架构的严重缺陷，它会发送极大量的网络流量到受害者系统，以便耗尽资源并降低公共服务的质量。因此，位于 SDN 架构上层的安全应用需要处理大量的流量信息，由于资源枯竭和性能瓶颈，系统可能会崩溃。因此，在大型 SDN 模型中，高流量情况下，为

收稿日期：2018-06-22；**修回日期：**2018-08-09　**基金项目：**国家自然科学基金资助项目（61572028）；广东省应用型科技研发专项资金项目（2016B020244003）；广东科贸职业学院院级优质专业核心课程网络工程综合设计（2015YZ-05）

作者简介：汪海涛（1978-），男，湖北宜城人，副教授，硕士，主要研究方向为计算机网络工程、下一代互联网和软件定义网络（wht1217@126.com）；余松森（1972-），男，江西丰城人，教授，硕导，博士（后），主要研究方向为物联网、大数据和软件定义网络.

了降低运行在上层的安全应用的巨大性能压力，数据层需要支持更高级的功能。

为解决以上问题，提高大型 SDN 模型的鲁棒性，本文提出了一种基于聚类算法和分布式自组织映射的软件定义网络系统。在这个提出的方案中引入聚类算法和 DSOM 机制，并让安全模块分布在 OpenFlow 交换机上，而不是分布在控制层或应用层，这些模块由分布式系统控制器控制，在 SDN 架构的应用层作为安全应用运行。此外，在 OpenvSwitch 中实现了扩展模块，允许连接到 OpenvSwitch 的默认代理，以实现统计、修改规则以及与分布式系统控制器进行通信的目的

1 相关工作

1.1 软件定义网络和 OpenFlow 协议

软件定义网络（SDN）为未来提供了一个有前景的网络架构。在该网络中，位于 SDN 控制器中的控制层与数据层是分离的。运行在应用层上的应用可以提供复杂的网络服务和功能。数据层处理硬件级别，并侧重于基于控制器配置的数据包处理。控制层（SDN 控制器）和数据层（OpenFlow 交换机）之间的通信由 OpenFlow 协议定义。在交换消息之前，OpenFlow 交换机必须建立到 SDN 控制器的安全连接以进行认证。该协议使控制器能够访问 OpenFlow 交换机中的流表，以使用安全连接进行控制、配置和统计[7,8]。

1.2 K-均值聚类

K-均值聚类[9,10]属于典型的启发式的算法，在聚类过程中，将 n 个数据对象分成 K 个簇，使得每个簇内的对象具有高度相似，而不同簇之间具有低度相似性。首先，算法从所有 n 个对象中选出 K 个，以此为初始聚类中心，其余对象以自身到不同聚类中心的距离为标准，加入到最相近的类中。然后，算法更新各个类的中心，不断重复上述过程，直到得出理想的簇集。

1.3 自组织映射算法

自组织映射（Self-Organization Mapping ，SOM）[11]是人工神经网络中的无监督学习方案之一。该算法将高维输入空间转换为低维表示，称为 SOM 映射。SOM 根据两种主要模式（训练和映射）分类或检测新的输入向量。训练过程使用输入样本建立、重新组织映射，而映射过程通过在映射中找到其获胜的神经元或节点，自动分类新的输入向量。

定义以下参数：

a） N 为迭代次数或训练样本 $\left[\vec{x}_1,\ldots,\vec{x}_N\right]$ 数量。

b）映射有 S 个神经元，每个神经元由一个向量 W 组成，W 由 w 个权重值组成。

c） R 是矩形映射的半径，其定义为：

$$R=\frac{\max(MapWidth,MapHeight)}{2} \tag{1}$$

d） λ 是一个时间常数，计算公式为：

$$\lambda=\frac{N}{\lg(R)} \tag{2}$$

e） $\sigma(t)$ 是获胜神经元（最佳匹配单元）的近邻半径，并随着时间的推移逐渐减小。假设近邻保持以同一个神经元为中心，实际上最佳匹配单元将根据下面的步骤 b)中的计算公式来移动。在算法的第 t 次迭代中， $\sigma(t)$ 计算公式为

$$N\sigma(t)=R\times\exp\left(-\frac{t^2}{\lambda}\right),t=1,\ldots,N \tag{3}$$

自组织映射算法的主要步骤如下：

a）初始化。用随机值或固定值初始化神经元的 m 维权重：$W_i=[W_{i1},W_{i2},W_{i3},\ldots,W_{iw}]$，其中 $1\le i\le S$。

b）选择最佳匹配单元（BMU）。输入向量 $x_k=[x_{k1},x_{k2},x_{k3},\ldots,x_{kw}]$，通过计算输入向量到所有神经元 i 的欧几里得距离 D_{ist}，从而把输入向量馈送到映射中。

$$D_{ist}=\sqrt{\sum_{j=1}^{w}\left(x_{kj}-W_{ij}\right)^2} \tag{4}$$

为输入向量 x_k 选择距离 D_{ist} 最小的神经元作为最佳匹配单元。

c）更新 BMU 的近邻权重：按照等式（3）计算 BMU 的近邻。之后，根据以下等式调整这些近邻的权重，进行下一次迭代，以使它们更接近输入向量。

$$W(t+1)=W(t)+L(t)*\Theta(t)*(x_k(t)-W(t)) \tag{5}$$

其中: $L(t)$ 是学习率，随着时间的推移也会衰减，计算公式为

$$L(t)=L_0*\exp\left(-\frac{t}{\lambda}\right) \tag{6}$$

$\Omega(t)$ 是邻近神经元与 BMU 的距离对其学习的影响量,定义为

$$\Omega(t)=\exp\left(-\frac{D_{ist}^2}{2\sigma^2(t)}\right) \tag{7}$$

d）循环：重复步骤（b）c），直到没有更多的输入向量馈送到映射。

1.4 SDN 视角下的泛洪攻击

在传统的网络架构中，泛洪攻击一般分为两类：带宽耗尽攻击和资源耗尽攻击。在带宽耗尽攻击中，攻击者往往用不受欢迎的流量淹没受害者网络，目的是耗尽受害者网络的带宽。这导致正常流量无法正常访问受害者系统，如 ICMP 泛洪、UDP 泛洪或 Smurf 和 Fraggle 攻击等。在资源耗尽攻击中，攻击者希望将异常 IP 数据包或误用的网络协议数据包发送给受害者。因此，每当开放连接的数量达到系统阈值时，受害者网络就会遭受资源耗尽，并可能停止工作[12]。

2 分布式网络流量攻击检测方法

2.1 系统概述

在大规模软件定义网络中，为了处理网络系统受到泛洪攻击时的性能瓶颈问题，引入了基于聚类算法的分布式 SDN 系统。图 1 显示了所提出的系统概览，所有交换机都在 SDN 控制

器的控制下运行。在应用层中，放置一个叫做 DSOM 控制器的应用程序来控制 DSOM 操作。

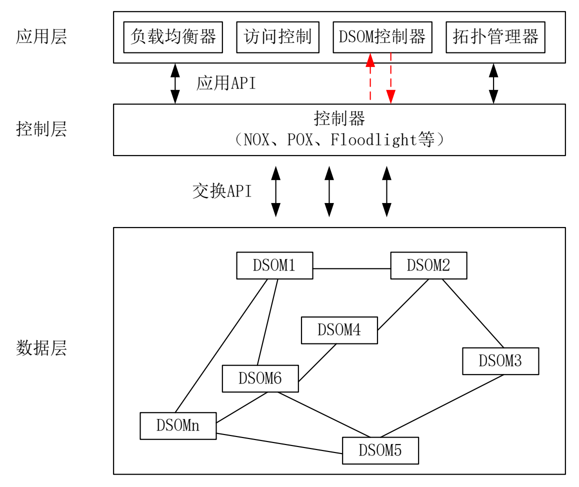


图 1　提出的分布式 SOM 系统

2.2　系统工作流程

引入的 DSOM 系统设计有四个主要过程：

a）初始化。位于应用层的 DSOM 控制器将现成的数据集发送给集成了 DSOM 扩展包的交换机。在每个交换机上，使用从控制器接收到的数据集来训练 DSOM 映射。

b）合并 DSOM。此阶段负责在预定时间内合并 DSOM。DSOM 控制器从 OpenFlow 交换机收集 DSOM 映射，生成合并的 SOM 映射，表示为

$$MergedMap = \sum_{j=1}^{j=n} \frac{\chi_j}{\sum_{i=1}^{i=n} \chi_i} \times MapDSOM_j \tag{8}$$

其中：χ_j 是第 j 个 DSOM 的训练输入样本总数，$MapDSOM_j$ 是第 j 个 DSOM 的映射。

c）更新。DSOM 控制器将合并的 SOM 映射发送到所有的 OpenFlow 交换机。合并的 SOM 映射替换 $DSOM_j$ 映射，以在交换机上继续分类过程。

d）分类。 $DSOM_j$ 根据他们的神经元对输入进行计算并给出结果，然后将这些结果发送到 DSOM 控制器作进一步的决定。

2.3　DSOM 交换机层

在交换机层，为 OpenFlow 交换机添加了一些附加模块，称为 DSOM 扩展模块：流收集器、特征提取器、训练数据库、DSOM 映射、快速策略实施和 DSOM 交换机代理。图 2 显示了这些模块是如何连接的，以及如何与 OpenFlow 交换机的默认模块一起工作。DSOM 交换机代理充当本地交换机层 DSOM 系统的核心，并控制 DSOM 映射过程的训练和更新，将分类结果发送到快速策略实施和 DSOM 控制器。

在初始化步骤中，从 DSOM 控制器发送的训练数据集通过 OpenFlow 交换机的 OpenFlow 通道到达 DSOM 交换机代理。然后转发到训练数据库，并且成为 DSOM 映射的训练输入。当训练过程完成后，DSOM 交换机代理向 DSOM 映射、特征提取器以及流收集器发送启动命令，以启动这些模块。如该方案的工作原理一样，流量收集器周期性地向交换机数据层发送统计消息，以在特征提取阶段获取单独的流量信息，该阶段侧重于通过交换机的每个用户的特征提取。此外，由特征提取器的输出更新训练数据库，并且在由 DSOM 交换机代理设置的时间段内再次调用训练 DSOM 映射过程。这种训练使 DSOM 映射能够适应即将到来的流量，并提高了每个本地 DSOM 交换机的分类性能。

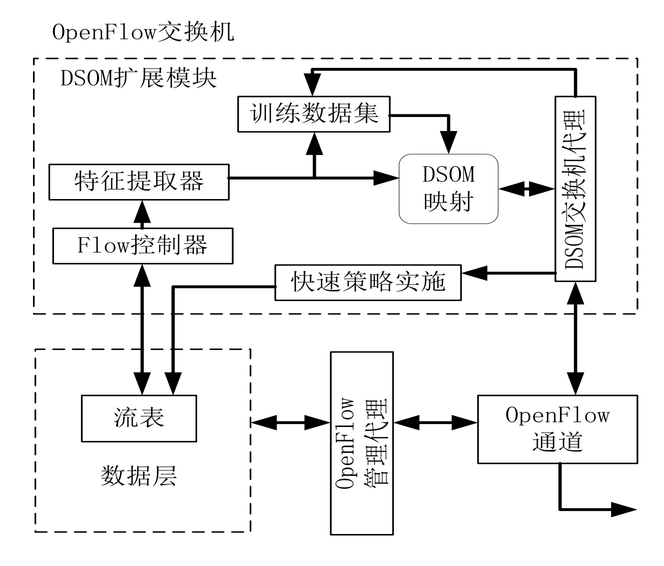


图 2　DSOM 交换机层

让更详细地了解特征提取器，以了解在 DSOM 映射的输入中使用了多少特征。对于每种类型的网络流量，这些特征可以是多样的；但是，正如前文所述，从 SDN 角度考虑普通的泛洪攻击，并将其分为两种主要类型：带宽耗尽攻击和资源耗尽攻击。因此，本文工作主要集中在两种类型的泛洪攻击，的方法是在预定的时间内观察每个用户。DSOM 映射与单个 SOM 执行相同的操作。它确定哪些用户是正常的用户哪些用户是异常的用户。为了作出最后的决定，将 K-均值聚类算法应用到系统中，将 n 个模式划分为 K 个聚类。在攻击用户被明确定义之后，DSOM 映射将用户信息发送到 DSOM 交换机代理，然后这个代理通过 OpenFlow 通道将这些数据传送到快速策略实施和 DSOM 控制器。在交换机上放置快速策略实施模块的目的是，通过在流表中设置直接的规则来对攻击流量进行快速反应，而位于 DSOM 控制器中的策略检查模块则负责验证规则，并且如果需要的话它可以覆盖规则。

3　实验

3.1　数据集和攻击模拟器

3.1.1 训练和测试数据集

从 CAIDA[13]、NSL-KDD[14]和 DARPA[15]这三个数据集中分析和构建了一套 SOM 训练样本和测试样本。这些数据集的简短描述总结如下：

CAIDA 数据集可用于 Web、FTP、Ping 等多种不同类型流量的混合研究。从表 1 的描述来看，通常情况下，TCP 和 ICMP 协议构成网络流量的比例最高。

表 1　以字节为单位统计的 CAIDA 数据集

流量状态	TCP（%）	ICMP（%）	其他（%）
正常	88.45	6.0	5.55
攻击型	7.58	91.25	1.17

对于 NSL-KDD 数据集，只研究 DoS 攻击。因此，只考虑使用 DoS 样本来训练和测试所提出的系统，如表 2 所示。

表 2　NSL-KDD 数据集中的 Dos 攻击

Dos 攻击类型	训练模式	测试模式	特征数量
back land neptune pod smurf teardrop	45927	7458	41

从三个数据集的 pcap 文件中提取并随机选择样本（包括正常和攻击模式）进行测试。

3.1.2 攻击模拟器

利用 BoNeSi 进行测试，BoNeSi 不仅可以模拟僵尸网络的流量，还可以通过定义的僵尸网络向目标网络或指定的 IP 地址生成 TCP、ICMP 或 UDP 泛洪攻击。

3.2　SDN 中的系统设置

实验测试的网络拓扑连接如图 3 所示，使用一个控制器（Controller）、四个与 DSOM 模块集成的 OpenvSwitch（DSOM OpenvSwitch）、一个网络服务器以及三个主机（h1，h2，h3，h4）作为流量发生器。表 3 给出了 DSOM 映射的详细参数。另外，由于大部分用户的访问是正常、合法的，本文设置聚类中心的数目为 4，以便构成正常用户的集合。

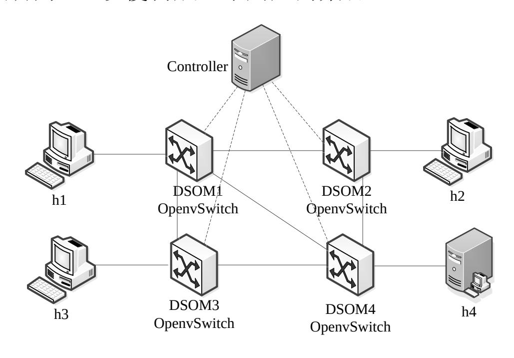


图 3　DSOM 实现的拓扑结构

表 3　SOM 映射参数

参数	值
半径	（宽度+高度）/2
学习速率	0.1
神经元数量	400，900，1600
输入维度	6
输出维度	2

3.3　系统测试

3.3.1 性能瓶颈测试

为了评估提出的系统在性能瓶颈方面与单个 SOM 相比取得的效果，建立了如图 3 所示的系统，并进行了两个测试实例：单个 SOM 和 DSOM 系统。在第一个测试场景中，在控制器中实现了一个 SOM 模块，其中控制器包含四个功能：流量收集器、特征提取器、SOM 映射、策略实施。同时，在所提出的系统中，只将 DSOM 控制器模块作为 SDN 控制器中的应用运行，其他模块在交换机中实现。在这两个实例中，使用了总共 12000 个样本的同一个数据集来训练 SOM 映射，其中从每个数据集随机提取了 4000 个模式。然后使用 BoNeSi 工具生成两个流量级别（50 Mbps 和 100 Mbps）来攻击网络服务器，并在两种情况下测量 SDN 控制器的 CPU 利用率。

3.3.2 SOM 性能测试

对于介绍的解决方案中 SOM 映射的性能检测，进行了以下设置实例来评估 DSOM 系统，并证明所提出的方法与传统的 SOM 机制具有相同的性能：

单一 SOM：一个单一的 SOM，四个与第 3.3.1 节中描述的相同模块。控制器从 OpenvSwitch 收集流量信息，然后检测攻击用户。如果检测到异常用户，策略实施会立即将规则应用于 OpenvSwitch。

DSOM 1：1：1：这个情况是在提出的 DSOM 系统中进行的，初始化过程中训练数据集的比例是 1：1：1。

• DSOM 1：2：3：这种情况与前一情况相同，只是初始化过程中训练数据集的比例为 1：2：3。

在这个实验中，分别对每种情况进行以下测试：

如表 4 所示，SOM 映射初始化和训练过程在单独的数据集（CAIDA，NSL-KDD 和 DARPA）上进行。然后，通过来自训练数据集的 5 次交叉验证执行测试程序，使用来自 BoNeSi DDoS 模拟器的流量进行测试。

通过随机合并三个相同的数据集而产生的混合数据集对 SOM 映射进行初始化和训练。并且，测试过程也由 5 次交叉验证以及 BoNeSi DDoS 模拟器执行。

对 SOM 映射中不同值的神经元数量：400,900 和 1600，进行了多次测试过程。

表 4 用于 SOM 检测性能测试的训练和测试样本

实例		单个 SOM	DSOM 1:1:1	DSOM 1:2:3
初始化		4000	4000:4000:4000	4000:4000:4000
训练		6000	2000:2000:2000	1000:2000:3000
测试	CAIDA 数据集	30000	30000	30000
	NSL-KDD 数据集	30000	30000	30000
	DARPA 数据集	30000	30000	30000
	混合数据集	30000	30000	30000
	BoNeSi 工具	6000	6000	6000

4　性能评估

4.1　处理性能瓶颈

图 4 所示为 SDN 控制器的 CPU 利用率，从图中可以看出，在测试实例之间存在显著差异，单个 SOM 机制总是消耗 SDN 控制器更多 CPU 资源，而 DSOM 系统则使控制器系统消耗的 CPU 资源处于稳定水平。在产生流量是 50 Mbps 的实例中，在攻击发起后仅 12 秒和 33 秒，CPU 利用率的值就达到 40%和 60%。同时，DSOM 解决方案在所有测试时间内仅占用约 23%的 CPU 资源。在 100Mbps 的情况下也可以看出同样的差别：单个 SOM 方案在仅仅 10 秒之后 SDN 控制器的 CPU 利用率就达到了 60%，并且在测试结束之前一直在这个值上下波动。相比之下，DSOM 解决方案在 CPU 的占用方面一直保持较低水平。

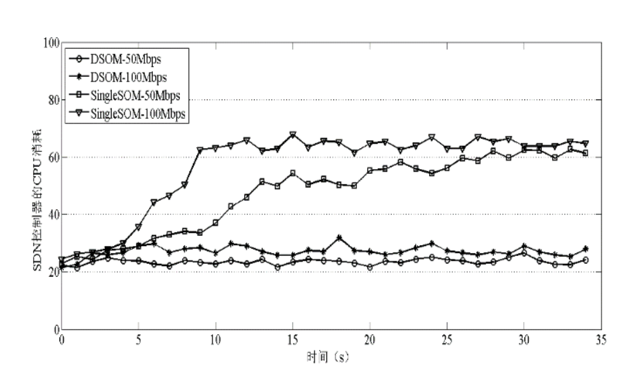


图 4　SDN 控制器的 CPU 消耗

从以上结果可以看出，DSOM 系统是完全胜过单一 SOM 方案的很好的一个解决方案。在单个 SOM 情况下，为了获取流量信息，控制器必须频繁地向交换机发送信息，然后将其转发到下一个模块，以便进一步处理。而且，同时处理来自所有边缘交换机的流量信息对于模块来说是一项繁重的工作。而 DSOM 系统将流量处理任务委派给边缘交换机以减少工作量，仅在策略检查时处理少量信息。另外，每个边缘交换机只处理从外部网络进入其端口的流量。因此，与单个 SOM 方案相比，DSOM 交换机代理的压力并不大。

4.2　SOM 性能评估

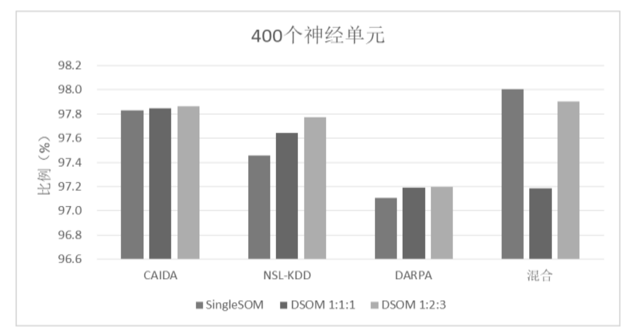
在评估 DSOM 方法的性能之前，本文作出如下定义：TP 表示攻击用户被分类为攻击用户的概率，TN 表示正常用户被认为是正常用户的概率，FP 表示异常用户被认为是正常用户的概率，FN 表示正常用户被认定为攻击用户的概率。

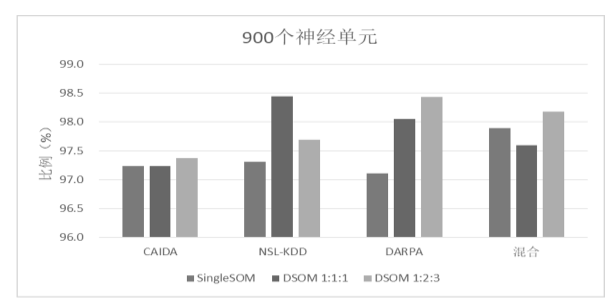
4.2.1 检测率

为了评估所提出的 DSOM 系统的效率，考虑了一个关键的标准，即检测率。检测率计算如下：

$$DR = \frac{TP}{TP + FN} \tag{9}$$

图 5 显示了对不同的四个数据集，在三种情况下 SOM 映射的检测率。从图中可以看出，在相同数量的神经元下，三种情况在所有四个数据集中只有轻微的差异。这是因为使用均值聚类算法来区分正常用户和异常用户，并使用 k 倍交叉验证技术来评估数据集本身的检测率。然而，即使使用攻击工具来产生流量，由于训练样本数量很大，训练好的 SOM 也可以很容易地检测到攻击用户。此外，这些实验还表明，如果 SOM 映射具有更多的神经元，这意味着检测性能更高，并且所提出的 DSOM 和单个 SOM 系统相比，没有太大差异。





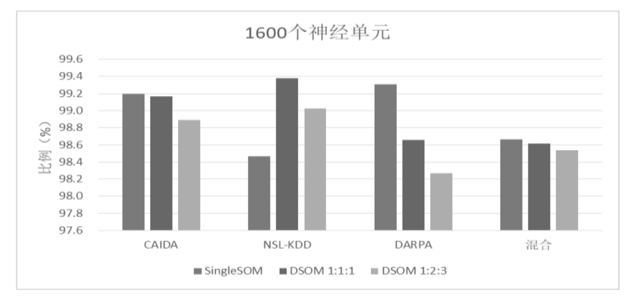


图 5　在三种不同神经元数量、四个不同数据集情况下，SOM 映射的检测率

4.2.2 准确性

准确度[16]即 SOM 映射作出决定的准确程度，计算公式为：

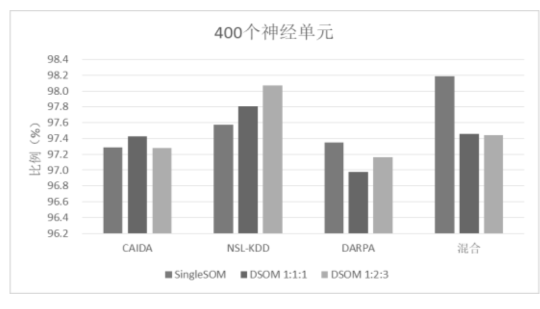
$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{10}$$

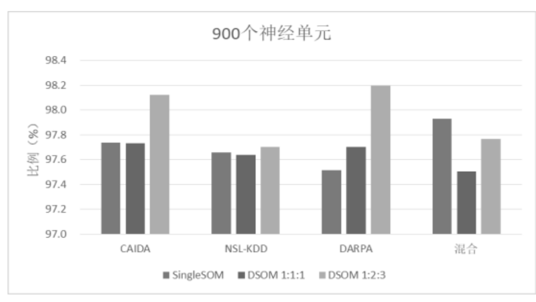
图 6 显示了对不同的四个数据集，在三种情况下 SOM 映射的准确度，三个实验的准确性均比较高。在 400 个神经元的情况下，最低的准确率约为 96.9%，而在 900 和 1600 个神经元的情况下，它的准确率都在 97%以上。原因在于，当 SOM 映射的学习样本数目增加时，对用户作出决定的准确性也更准确。而且，当 SOM 映射达到可以作出完全准确决定的阈值时，神经元的数量对准确性的影响不大。这就是为什么在精度方面这些测试之间只有微小的差别。

4.2.3 系统开销

还通过测量两个系统的处理时间和分类时间，来评估 DSOM 机制和单个 SOM 的性能。对于 DSOM 系统，假设通过数据包连接传输数据所需的时间仅为几毫秒，则处理时间主要

是通过两个过程的和来计算：第一个是在 OpenvSwitch 上训练 DSOM 映射，它占用了最多的时间，第二是在 DSOM 控制器上的合并时间。同时，单个 SOM 的处理时间只是其训练时间。用输入集训练 DSOM 和单个 SOM 映射，如表 5 所示。





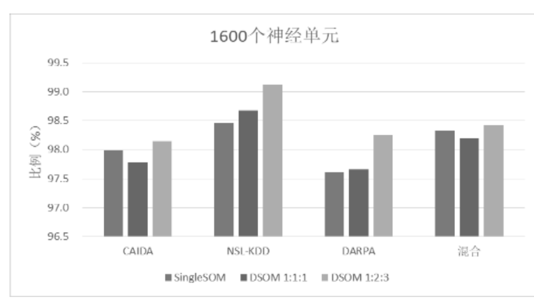


图 6 在三种不同神经元数量、四个不同数据集情况下，SOM 映射的准确性

表 5 中的结果表明，如果在 SOM 映射中使用更多数量的神经元，则 DSOM 系统的处理时间比单个 SOM 更快。因为 OpenvSwitch 的 DSOM 使用较小的数据集进行训练，而单个 SOM 总是需要更大的输入数据集来训练其映射。关于分类时间，三种情况大致相等，并且与神经元数量成正比增加。这可以通过对控制器和 OpenvSwitch 使用相同的配置来解释；因此，这三种情况下的 CPU 处理时间没有太大的差别。

表 5 处理时间和分类时间

神经元数量	实例	处理（s）	分类（ms）
	单个 SOM	10.14	0.956
400	DSOM 1:1:1	9.16	0.932
	DSOM 1:2:3	9.81	0.895
	单个 SOM	25.95	1.82
900	DSOM 1:1:1	15.71	1.81
	DSOM 1:2:3	18.04	1.70
	单个 SOM	37.77	4.55
1600	DSOM 1:1:1	23.99	4.03
	DSOM 1:2:3	28.72	4.45

根据以上实验结果，可以评估软件定义网络中 DSOM 系统的性能，并且与单个 SOM 进行比较。首先，在处理性能瓶颈问题和方面，DSOM 系统是一个很好的解决方案，完全胜过单一 SOM 方案。而且，这两个系统对异常流量的检测率和准确率方面都表现出优异的性能。在使系统准备好分类过程的开销方面，所提出的 DSOM 比使用单个 SOM 要少。总的来说，软件定义网络中的 DSOM 系统能够有效地解决大型网络中泛洪攻击下的瓶颈问题，与传统方法相比具有一定的优势。

5 结束语

本文提出了一种 K-均值聚类算法和分布式自组织映射系统，通过使用分布式系统而不是集中式的系统对网络数据进行分析，处理由于大型软件定义网络中上层泛洪攻击引起的聚合而导致的瓶颈问题。实验结果表明，在处理性能瓶颈方面，本文所提出的方法完全胜过传统的方法。此外，实验结果不但显示了的机制与单个 SOM 系统的性能相同，而且表明了 DSOM 系统的开销要优于单个 SOM。

参考文献：

[1] 胡涛，张建辉，毛明. SDN 中基于迁移优化的控制器负载均衡策略 [J]. 计算机应用研究, 2018, 35 (2): 559-563. (Hu Tao, Zhang Jianhui, Mao Ming. Controller load balancing strategy based on migration optimizing in SDN [J]. Application Research of Computers, 2018, 35 (2): 559-563.)

[2] 邱欣逸，李俊，周建二，等. OpenFlow 中基于精确时间戳的延迟测量方法 [J]. 通信学报, 2017, 38 (11): 178-187. (Qiu Xinyi, Li Jun, Zhou Jianer, *et al.* New delay measurement method based on accurate timestamp in OpenFlow [J]. Journal on Communications, 2017, 38 (11): 178-187.)

[3] Wang Haopei, Xu Lei, Gu Guofei. FloodGuard: A DoS Attack Prevention Extension in Software-Defined Networks [C]// Proc of International Conference on Dependable Systems and Networks. Washington DC: IEEE Computer Society, 2015: 239-250.

[4] Jain S, Kumar A, Mandal S, *et al.* B4: experience with a globally-deployed software defined wan [J]. Computer Communication Review, 2013, 43 (4): 3-14.

[5] 王启林，李小鹏，郁滨，等. 基于连接认证的低功耗蓝牙泛洪攻击防御方案 [J]. 计算机应用研究, 2017, 34 (2): 499-502. (Wang Qilin, Li Xiaopeng, Yu Bin, *et al.* Defense scheme of flooding attacks in bluetooth low energy based on connection authentication [J]. Application Research of Computers, 2017, 34 (2): 499-502.)

[6] 张永铮，肖军，云晓春，等. DDoS 攻击检测和控制方法 [J]. 软件学报, 2012, 23 (8): 2058-2072. (Zhang Yongzheng, Xiao Jun, Yun Xiaochun, *et al.* DDoS attacks detection and Control mechanisms [J]. Journal of Software, 2012, 23 (8): 2058-2072.)

[7] Lara A, Kolasani A, Ramamurthy B. Network innovation using openflow: a survey [J]. IEEE Communications Surveys & Tutorials, 2014, 16 (1): 493-512.

[8] Jafarian J H, Al-Shaer E, Duan Qi. Openflow random host mutation:

transparent moving target defense using software defined networking [C]// Proc of Workshop on Hot Topics in Software Defined Networks. New York: ACM Press, 2012: 127-132.

[9] Sulaiman S N, Nor Ashidi Mat Isa. Adaptive fuzzy-K-means clustering algorithm for image segmentation [J]. IEEE Trans on Consumer Electronics, 2010, 56 (4): 2661-2668.

[10] 张顺龙，库涛，周浩. 针对多聚类中心大数据集的加速 K-means 聚类算法 [J]. 计算机应用研究, 2016, 33 (2): 413-416. (Zhang Shunlong, Ku Tao, Zhou Hao. Accelerate K-means for multi-center clustering of big datasets [J]. Application Research of Computers, 2016, 33 (2): 413-416.)

[11] 吴怡，杨琼，吴庆祥，等. 基于自组织映射神经网络的 VANET 组网算法 [J]. 通信学报, 2011, 32 (12): 136-145. (Wu Yi, Yang Qiong, Wu Qingxiang, *et al.* Networking algorithm based on self-organizing map neural network for VANET [J]. Journal on Communications, 2011, 32 (12): 136-145.)

[12] 章曙光，周学海，杨峰，等. 无线传感器网络中基于邻居节点信息的溯源追踪策略 [J]. 小型微型计算机系统, 2015, 36 (3): 483-487. (Zhang Shuguang, Zhou Xuehai, Yang Feng, *et al.* Traceback Mechanism Based on Neighbor Information in Wireless Sensor Networks [J]. Journal of Chinese Computer Systems, 2015, 36 (3): 483-487.)

[13] Wen Yuhao, Wang Han, Chen Zhen, *et al.* MASC: A bitmap index encoding algorithm for fast data retrieval [C]// Proc of IEEE International Conference on Communications. 2016: 1-6.

[14] KumarShrivas A, Dewangan A K. An Ensemble Model for Classification of Attacks with Feature Selection based on KDD99 and NSL-KDD Data Set [J]. International Journal of Computer Applications, 2014, 99 (15): 8-13.

[15] Moustafa N, Slay J. Creating novel features to anomaly network detection using DARPA-2009 data set [C]// Proc of European Conference on Cyber Warfare and Security Eccws. 2015: 23-24.

[16] 叶剑锋，王化明. AdaBoost 检测结合 SOM 的自动人脸识别方法 [J]. 哈尔滨工程大学学报, 2018, 39 (1): 129-134. (Ye Jianfeng, Wang Huaming. An automatic face recognition method using AdaBoost detection and SOM [J]. Journal of Harbin Engineering University, 2018, 39 (1): 129-134.)